Available online at www.sciencedirect.com
SCIENCE DIRECT®
Finite Fields and Their Applications 10 (2004) 1–23
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Uniform distribution of linear recurring sequences modulo prime powers

Tamás Herendi*,[1]

Institute of Mathematics and Informatics, University of Debrecen, Debrecen 4010, Hungary

Received October 5, 1999; revised July 15, 2002; accepted July 26, 2002

Communicated by Harald Niederreiter

Abstract

Let p be a prime, u be a linear recurring sequence of integers of order d and let $S = \frac{3d^2+9d}{2} + 1$. The main result of the present paper: if u is uniformly distributed mod p^S, then it is uniformly distributed mod p^s for all $s \geqslant 1$. This solves a longstanding folklore conjecture.

1. Introduction

Let $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ and $u = \{u_n\}_{n=0}^{\infty}$ be a sequence satisfying the recurrence relation

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n$$

for $n = 0, 1, \ldots$. Then u is called a *linear recurring sequence* (for short l.r.s.) with defining coefficients $a_0, \ldots, a_{d-1}$ and initial values $u_0, \ldots, u_{d-1}$.

The integer d is called the *order* of the recurrence and the polynomial

$$P(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

is called a *characteristic polynomial* of u.

* Fax: +36-52-310936.
E-mail address: herendi@math.klte.hu.
[1] Research supported in part by 016791 from the Hungarian National Foundation for Scientific Research and by the Universitas Foundation of Kereskedelmi Bank RT.

1071-5797/03/$ - see front matter
PII: S1071-5797(02)00007-2

Let $d(u)$ be the smallest integer for which there exists a recurrence relation of order $d(u)$ for the sequence u. This number is said to be the *minimal order* of the recurring sequence and the corresponding characteristic polynomial is said to be the *minimal characteristic polynomial* of u, which is unique by page 33 of [16].

Let $m, p \in \mathbb{N}$ and p be a prime. Then the p-adic valuation $v_p(m)$ is defined by: $m = p^{v_p(m)}m'$ where $\gcd(p, m') = 1$.

Let u be a l.r.s. and set $\delta(u) = \det A$, where $A \in \mathbb{Z}^{d(u)\times d(u)}$ with entries $a_{i,j} = u_{i+j-2}$. $\delta(u)$ will be called the *Hankel determinant* of u.

Let u be a sequence of integers and let $m \geqslant 2$ be an integer. We say that u is *periodic* mod m, if there exist μ_0, $\mu \in \mathbb{N}$ such that $u_{n+\mu} \equiv u_n \bmod m$ for all $n \geqslant \mu_0$. The smallest $\mu_0 = \mu_0(u, m)$ and $\mu = \mu(u, m)$ with the previous property will be called the *preperiod* and *minimal period length* of $u \bmod m$, respectively.

If $\mu_0(u, m) = 0$ then u is said to be *purely periodic* mod m.

Let u be a l.r.s. A simple observation shows that u is periodic mod m for any $m \geqslant 2$.

Let u be a sequence of integers. We will say that u is *uniformly distributed* (for short u.d.) mod m if

$$\lim_{N\to\infty} \frac{1}{N} \#\{n \leqslant N \mid u_n \equiv a \bmod m\} = \frac{1}{m}$$

for all $a \in \mathbb{Z}$.

It is easy to see that if u is u.d. mod m, then it is u.d. mod l for every $l|m$.

Let u be a l.r.s. of integers, defined by the coefficients $a_0, \ldots, a_{d-1}$ with initial values $u_0, \ldots, u_{d-1}$ and let p be a prime. Denote by

$$\bar{u}_n(k) = (u_{n+k-1}, u_{n+k-2}, \ldots, u_n)^{tr},$$

the nth k-dimensional state vector and by

$$M(u) = \begin{pmatrix} a_{d-1} & a_{d-2} & \cdots & a_1 & a_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

the companion matrix of u. We have with these notations $\bar{u}_n(d) = M(u)^n \bar{u}_0(d)$, which will be used frequently in the paper. Further let $d_p(u, s)$ be the minimal order, $\mu_p(u, s)$ be the minimal period length, $M_p(u, s)$ the companion matrix and $a_{s,0}, \ldots, a_{s,d(u,s)-1}$ the defining coefficients corresponding to the minimal recurrence relation of $u \bmod p^s$.

As far as there is no confusion, we will simplify our notation by omitting unnecessary parameters.

For further properties of linear recurring sequences we refer to [10].

The properties of linear recurring sequences were investigated by several authors from different viewpoints. One field of study is the periodicity of a l.r.s. reduced mod m. Ward [22] could prove that if u is a third order l.r.s and $m_1, m_2 \geqslant 2$ such that $\gcd(m_1, m_2) = 1$, then $\mu(u, m_1 m_2) = \mu(u, m_1)\mu(u, m_2)$. He also proved that u is purely periodic mod $m_1 m_2$ if and only if it is purely periodic both mod m_1 and mod m_2. Furthermore, he proved some results on the properties of the period length. Unfortunately in the proof of his Theorem 7.1 he forgot about the condition he used in his previous results, namely that the observed l.r.s. should be non-singular mod m. Non-singularity in his paper means that the Hankel determinant of the sequence and m should be relatively prime. (His Theorem 7.1 is about the period length of a l.r.s. modulo a prime power and contradicts our results.) In [23] he gave some results on the number of appearances of the residue classes of a third order l.r.s. Later in [24] he generalized in a correct form his results in [22] to linear recurrences of arbitrary order. Duparc [7,8] investigated the period length of general linear recurring sequences reduced to finite residue classes over unique factorization domains. Bundschuh and Shiue [3] generalized the result of Bundschuh [4] and gave a sufficient condition on the uniform distribution of general second order linear recurring sequences reduced modulo prime powers. Niederreiter [13] proved that the Fibonacci sequence is uniformly distributed mod m if and only if $m = 5^s$. Nathanson [12] gave a criterion for the uniform distribution of a second order l.r.s. mod primes. Webb and Long [25] characterized the general second order linear recurring sequences to be u.d. reduced modulo prime powers, and Bumby [2] with respect to general moduli. Niederreiter and Shiue [14,15] gave necessary and sufficient condition for a l.r.s. of order <5 to be uniformly distributed over finite fields. Here they proved that a general l.r.s. could be u.d. over a finite field only if its characteristic polynomial had a multiple root over the same field. This leads to the observation, that over the integers, a l.r.s. can be u.d. mod p (and thus mod p^s) only if p divides the discriminant of its characteristic polynomial. Narkiewicz [11] gave an overview on the uniform distribution of linear recurring sequences and among others, he studied the uniform distribution of second-order linear recurring sequences in general residue class systems. Turnwald [20,21] gave a complete characterization of second- and third-order linear recurrences defined over Dedekind domains to be uniformly distributed in residue class systems with finite norm. Tichy and Turnwald [18] applied the previous result and gave a criterion for u.d. of third-order linear recurring sequences over the integers. Drmota and Tichy [6] gave a survey of the topic and proved uniform distribution and weak uniform distribution properties of several sort of recurring sequences.

We call attention to the fact that our result seems to be useful for the observation of a more general distribution property of linear recurring sequences, studied in [5,17]. The latter gives comprehensive results on stability for second-order linear recurring sequences modulo prime powers.

You can find a generalization of the results in this paper to Dedekind-domains in the author's Ph.D. thesis [9]

Now, we formulate our main result of the present paper:

Theorem. *Let $p\in\mathbb{Z}$ be a prime, $d\geqslant 2$ an integer, u a dth-order integer linear recurring sequence and $S=\frac{3d^2+9d}{2}+1$. If u is uniformly distributed* $\bmod p^S$ *then also uniformly distributed* $\bmod p^s$ *for any $s\in\mathbb{N}$.*

Remark. The problem is contained in a list of related questions in the paper of Tichy [19].

In the cases $d=2$ and 3 we know much better exact bounds for the value of S. By Bumby [2] and Ward [23], if $d=2$, then $S=2$. Further if we assume that $p\geqslant 5$, then $S=1$. By Tichy [19], if $d=3$, then $S=3$. If we exclude $p=2$, then $S=2$.

2. Preliminary lemmas

Let p be a fixed prime.

$\{b_1,\ldots,b_r\}=B\subset\mathbb{Z}^d$ is called *semi-independent* $\bmod p^s$ if $\lambda_1b_1+\cdots+\lambda_rb_r\equiv 0 \bmod p^s$ implies that $\lambda_i\equiv 0 \bmod p$ for $i=1,\ldots,r$. Otherwise it is called *strongly dependent*.

If $b_1,\ldots,b_r,\ b\in\mathbb{Z}^d$ and $0\not\equiv p^kb\equiv\lambda_1b_1+\cdots+\lambda_rb_r \bmod p^s$ for some $k\in\mathbb{N}$ such that either $\lambda_i\not\equiv 0 \bmod p$ for some $i\in\{1,\ldots,r\}$ or $k=0$, then b is said to be a *linear semi-combination* of $b_1,\ldots,b_r \bmod p^s$.

If $\{b_1,\ldots,b_r\}=B\subset\mathbb{Z}^d$ is semi-independent $\bmod p^s$ and for all $b\in\mathbb{Z}^d$, b is a semi-combination of $b_1,\ldots,b_r \bmod p^s$, then B is called a *semi-basis* of $\mathbb{Z}^d \bmod p^s$.

We keep the notion of independence, combination and basis to be understood in their usual sense.

Lemma 1. *For every d, $s\in\mathbb{N}$ there exists a basis (in the usual sense) of $\mathbb{Z}^d \bmod p^s$ and it has exactly d elements.*

Proof. See e.g. [1, Theorem 7.12, p. 104].

Lemma 2. (a) *Let $b_1,\ldots,b_r\in\mathbb{Z}^d$ be linearly dependent over $\mathbb{Z}$. Then they are strongly dependent* $\bmod p^s$, *for any s.*

(b) *Let $b_1,\ldots,b_d\in\mathbb{Z}^d$ be linearly independent over $\mathbb{Z}$. Then $b_1,\ldots,b_d$ are semi independent* $\bmod p^s$ *for any $s>v_p(\det(b_1,\ldots,b_d))$.*

Proof. (a) Let $\lambda_1,\ldots,\lambda_r\in\mathbb{Z}$ be such that $\lambda_1b_1+\cdots+\lambda_rb_r=0$ and $\gcd(\lambda_1,\ldots,\lambda_r)=1$. Then at least one of the λ_i is not divisible by p, and by definition, $b_1,\ldots,b_r$ are strongly dependent $\bmod p^s$, for any $s\in\mathbb{N}$.

(b) Suppose now that

$$s>v_p(\det(b_1,\ldots,b_d)). \tag{1}$$

Let $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$ be such that $\lambda_1 b_1 + \cdots + \lambda_d b_d \equiv 0 \bmod p^s$. This is equivalent to $\lambda_1 b_1 + \cdots + \lambda_d b_d = p^s b$, for some $b \in \mathbb{Z}^d$. If $b = 0$, then $\lambda_1 = \cdots = \lambda_d = 0$. Suppose, that $b \neq 0$. Since $b_1, \ldots, b_d$ are linearly independent over $\mathbb{Z}$, $\det(b_1, \ldots, b_d) \neq 0$, and Cramer's rule can be applied. Hence $\lambda_i \det(b_1, \ldots, b_d) = \det(b_1, \ldots, b_d | b_i = p^s b) = p^s \det(b_1, \ldots, b_d | b_i = b)$, for $i = 1, \ldots, d$. By (1), $p^s \nmid \det(b_1, \ldots, b_d)$. It follows, that $p | \lambda_i$ for all $i = 1, \ldots, d$. By definition this yields that $b_1, \ldots, b_d$ are semi independent $\bmod p^s$. □

Remark 1. If $r \neq d$ in Lemma 2(b), there still exists a lower bound on s with the same properties.

Corollary 1. *Let $b_1, \ldots, b_d \in \mathbb{Z}^d$ and $t = v_p(\det(b_1, \ldots, b_d))$. If $b_1, \ldots, b_d$ is not a semi-basis* $\bmod p^{t+1}$, *then not a semi-basis* $\bmod p^s$ *for any $s \in \mathbb{N}$.*

Proof. If $b_1, \ldots, b_d$ is not a semi-basis modulo p^{t+1}, then it is strongly dependent. By Lemma 2(b), this means that $b_1, \ldots, b_d$ are linearly dependent over $\mathbb{Z}$. Then by Lemma 2(a), we obtain the statement. □

Lemma 3. *If $b_1, \ldots, b_r \in \mathbb{Z}^d$ are semi-independent* $\bmod p^s$, *then $r \leqslant d$.*

Proof. By Lemma 2(a), $b_1, \ldots, b_r$ are independent over $\mathbb{Z}$, and thus independent over $\mathbb{Q}$ (using the natural embedding). □

Lemma 4. *If $b_1, \ldots, b_d \in \mathbb{Z}^d$ are semi-independent* $\bmod p^s$, *then $b_1, \ldots, b_d$ is a semi-basis* $\bmod p^s$.

Proof. Similarly as in the proof of Lemma 3, $b_1, \ldots, b_d$ is a basis of $\mathbb{Q}^d$. Thus for every $b \in \mathbb{Z}^d$ there exist $\lambda, \lambda_1, \ldots, \lambda_d \in \mathbb{Z}$ such that $\gcd(\lambda, \lambda_1, \ldots, \lambda_d) = 1$ and $\lambda b = \lambda_1 b_1 + \cdots + \lambda_d b_d$. Suppose that $v_p(\lambda) = k$ and $\lambda = \lambda' p^k$. There exists λ^- with the property $\lambda' \lambda^- \equiv 1 \bmod p^s$. Let $\lambda_i' = \lambda_i \lambda^-$ for $i = 1, \ldots, d$. Then

$$p^k b \equiv \lambda_1' b_1 + \cdots + \lambda_d' b_d \bmod p^s \tag{2}$$

and $\gcd(p^k, \lambda_1', \ldots, \lambda_d') = 1$. If $p^k b \equiv 0 \bmod p^s$ would hold, then $b_1, \ldots, b_d$ would be strongly dependent $\bmod p^s$, contrary to the assumption. □

Remark 2. Let $s < s'$ and suppose that $b_1, \ldots, b_d \in \mathbb{Z}^d$ is a semi-basis $\bmod p^s$. This $b_1, \ldots, b_d$ is also a semi-basis $\bmod p^{s'}$, otherwise it would be strongly dependent $\bmod p^{s'}$, which would yield $\lambda_1 b_1 + \cdots + \lambda_d b_d \equiv 0 \bmod p^{s'}$ for some $\lambda_1, \ldots, \lambda_d$ not all divisible by p. But then the same holds $\bmod p^s$ which would contradict the semi-independence of $b_1, \ldots, b_d$.

However more can be proved:

Lemma 5. *Let $s \leqslant s'$, $\{b_1, \ldots, b_d\} = B \subset \mathbb{Z}^d$ and suppose that B is a semi-basis* $\bmod p^s$. *If $b \in \mathbb{Z}^d$, then there exist $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$ such that* $p^{s-1}b \equiv \lambda_1 b_1 + \cdots + \lambda_d b_d \bmod p^{s'}$.

Proof. Doing the same steps as in the proof of Lemma 4 with the difference that we define λ^- by the congruence $\lambda'\lambda^- \equiv 1 \bmod p^{s'}$, we get that $k \leqslant s-1$. If we multiply both sides of (2) by p^{s-1-k}, we obtain the lemma. □

3. Lemmas on recurring sequences

Throughout this section we suppose, that the linear recurring sequences are purely periodic in the considered residue classes.

Let u be a l.r.s. of integers, p be a fixed prime and $s \in \mathbb{N}$. To simplify the notation introduced in Section 1 we put $d(u,s) = d_p(u,s)$, $\mu_0(u,s) = \mu_{0p}(u,s)$ and $\mu(u,s) = \mu_p(u,s)$.

Lemma 6. *Let $a, b \in \mathbb{Z}$ and u and v two linear recurring sequences with minimal characteristic polynomials P_u and P_v. Then $au + bv$ is also a linear recurring sequence, and its minimal characteristic polynomial divides* $\operatorname{lcm}(P_u, P_v)$.

Proof. The polynomial $\operatorname{lcm}(P_u, P_v)$ is a characteristic polynomial for both sequences u and v (see e.g. [21]) and thus a characteristic polynomial for all linear combinations of them. □

Remark 3. We may define $v_n = u_{n+k}$ for some $k \geqslant 0$. Then $P_v = P_u$.

If $M(u)$ and $M(v)$ are the companion matrices of P_u and P_v, respectively, let $M(u) * M(v)$ denote the companion matrix corresponding to $\operatorname{lcm}(P_u, P_v)$.

Lemma 7. (a) *With the definitions of Section 2, $\bar{u}_0(d(u,s)), \ldots, \bar{u}_{d(u,s)-1}(d(u,s)) \in \mathbb{Z}^{d(u,s)}$ form a semi-basis* $\bmod p^s$.

(b) *Let $0 < r \leqslant q$. If $\bar{u}_0(q), \ldots, \bar{u}_{r-1}(q) \in \mathbb{Z}^q$ are semi-independent* $\bmod p^s$, *then $r \leqslant d(u,s)$.*

Proof. (a) If $s = 1$, then the independence (and which is the same in this case, the semi-independence) follows from e.g. [10, Theorem 6.51, p. 214].

Throughout the proof of the lemma we will use the notation $\bar{u}_n = \bar{u}_n(d(u,s))$.

Let $s > 1$. Suppose that $\bar{u}_0, \ldots, \bar{u}_{d(u,s)-1}$ is not a semi-basis $\bmod p^s$, whence by Lemma 4, they are strongly dependent. This yields that there exists a set of coefficients $\lambda_0, \ldots, \lambda_{d(u,s)-1} \in \mathbb{Z}$ and $k \in \{0, \ldots, d(u,s)-1\}$ such that $\gcd(\lambda_k, p) = 1$ and

$$\lambda_0 \bar{u}_0 + \cdots + \lambda_{d(u,s)-1} \bar{u}_{d(u,s)-1} \equiv 0 \bmod p^s. \tag{3}$$

We claim that we may choose $\lambda_0, \ldots, \lambda_{d(u,s)-1}$ such that $\lambda_{d(u,s)-1} \equiv 1 \bmod p^s$. This is obvious if $k = d(u,s) - 1$.

On the contrary, suppose that $p|\lambda_{d(u,s)-1}$ for every system of $\lambda_0, \ldots, \lambda_{d(u,s)-1} \in \mathbb{Z}$ which satisfy (3).

Fix $\lambda_0, \ldots, \lambda_{d(u,s)-1} \in \mathbb{Z}$ satisfying (3) such that the corresponding k, given as before, is maximal.

For this k we have $k < d(u,s) - 1$. Multiplying (3) by $M(u,s)$, we get

$$\begin{aligned} 0 &\equiv M(u,s)\left(\lambda_0\bar{u}_0 + \cdots + \lambda_{d(u,s)-1}\bar{u}_{d(u,s)-1}\right) \\ &\equiv \lambda_0 M(u,s)\bar{u}_0 + \cdots + \lambda_{d(u,s)-1}M(u,s)\bar{u}_{d(u,s)-1} \\ &\equiv \lambda_0\bar{u}_1 + \cdots + \lambda_{d(u,s)-1}\bar{u}_{d(u,s)} \bmod p^s. \end{aligned} \tag{4}$$

By the definition of $d(u,s)$ there exist $a_{s,0}, \ldots, a_{s,d(u,s)-1}$ such that

$$a_{s,0}\bar{u}_0 + \cdots + a_{s,d(u,s)-1}\bar{u}_{d(u,s)-1} \equiv \bar{u}_{d(u,s)} \bmod p^s.$$

Substituting this into (4) we obtain

$$\begin{aligned} 0 \equiv{}& \lambda_0\bar{u}_1 + \cdots + \lambda_{d(u,s)-2}\bar{u}_{d(u,s)-1} \\ &+ a_{s,0}\lambda_{d(u,s)-1}\bar{u}_0 + \cdots + a_{s,d(u,s)-1}\lambda_{d(u,s)-1}\bar{u}_{d(u,s)-1} \bmod p^s. \end{aligned} \tag{5}$$

Set $\lambda'_0 = a_{s,0}\lambda_{d(u,s)-1}$ and $\lambda'_i = \lambda_{i-1} + a_{s,i}\lambda_{d(u,s)-1}$ for $i = 1, \ldots, d(u,s) - 1$. Since $p|\lambda_{d(u,s)-1}$, we have $\gcd(\lambda'_{k+1}, p) = 1$. By (5), $\lambda'_0, \ldots, \lambda'_{d(u,s)-1}$ is also a suitable choice for the coefficients to combine to 0, which contradicts the selection of k.

Choose $\lambda_0, \ldots, \lambda_{d(u,s)-1} \in \mathbb{Z}$ satisfying (3) such that $\lambda_{d(u,s)-1} \equiv 1 \bmod p^s$. Hence

$$-\lambda_0\bar{u}_0 - \cdots - \lambda_{d(u,s)-2}\bar{u}_{d(u,s)-2} \equiv \bar{u}_{d(u,s)-1} \bmod p^s.$$

Multiplying both side of the congruence by $M(u,s)^n$, we obtain

$$-\lambda_0\bar{u}_n - \cdots - \lambda_{d(u,s)-2}\bar{u}_{n+d(u,s)-2} \equiv \bar{u}_{n+d(u,s)-1} \bmod p^s,$$

which contradicts the definition of $d(u,s)$.

(b) On the contrary, suppose that $d(u,s) < r$. By the definition of $d(u,s)$ there exist integers $\lambda_0, \ldots, \lambda_{d(u,s)-1}$ such that

$$\bar{u}_{d(u,s)}(q) \equiv \lambda_0\bar{u}_0(q) + \cdots + \lambda_{d(u,s)-1}\bar{u}_{d(u,s)-1}(q) \bmod p^s,$$

which means that $\bar{u}_0(q), \ldots, \bar{u}_{r-1}(q)$ are strongly dependent. □

Since $d(u,s) \leqslant d(u)$ and $d(u,s) \leqslant d(u,s+1)$ for all $s \in \mathbb{N}$, there exists an integer T, such that $d(u,T) = d(u,s)$ for all $s \geqslant T$. The smallest such a T will be denoted by $T(u)$.

Lemma 8. *Let u be a l.r.s. and $q \geqslant d(u)$. Then the vectors $\bar{u}_0(q), \ldots, \bar{u}_{d(u)-1}(q)$ are independent over $\mathbb{Z}$.*

Proof. Let P be the minimal characteristic polynomial of u over $\mathbb{Z}$. Then obviously P is a minimal characteristic polynomial of u over $\mathbb{Q}$.

Let M be the q dimensional companion matrix of the sequence u, i.e. $\bar{u}_{n+1}(q) = M\bar{u}_n(q)$. Suppose that $\bar{u}_0(q), \ldots, \bar{u}_{d(u)-1}(q)$ are dependent over $\mathbb{Z}$. Then there exist $\lambda_0, \ldots, \lambda_{d(u)-1} \in \mathbb{Z}$ such that

$$\lambda_0\bar{u}_0(q) + \cdots + \lambda_{d(u)-1}\bar{u}_{d(u)-1}(q) = 0.$$

Let $0 \leqslant k \leqslant d(u) - 1$ be the largest index for which $\lambda_k \neq 0$. For this k we can write

$$-\frac{\lambda_0}{\lambda_k}\bar{u}_0(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}\bar{u}_{k-1}(q) = \bar{u}_k(q).$$

Multiplying this equation by M^n we obtain

$$\begin{aligned}
\bar{u}_{k+n}(q) &= M^n\bar{u}_k(q) \\
&= M^n\left(-\frac{\lambda_0}{\lambda_k}\bar{u}_0(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}\bar{u}_{k-1}(q)\right) \\
&= -\frac{\lambda_0}{\lambda_k}M^n\bar{u}_0(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}M^n\bar{u}_{k-1}(q) \\
&= -\frac{\lambda_0}{\lambda_k}\bar{u}_n(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}\bar{u}_{n+k-1}(q)
\end{aligned}$$

for any $n \geqslant 0$. But then $P' = x^k + \frac{\lambda_{k-1}}{\lambda_k}x^{k-1} + \cdots + \frac{\lambda_0}{\lambda_k}$ is again a characteristic polynomial of u over $\mathbb{Q}$, with degree less than $d(u)$. This is a contradiction, thus $\bar{u}_0(q), \ldots, \bar{u}_{d(u)-1}(q)$ are independent over $\mathbb{Z}$. □

Lemma 9. *Let u be a l.r.s. Then $d(u) = d(u, T(u))$.*

Proof. Clearly $d(u) \geqslant d(u, T(u))$. By Lemma 7(b), the $d(u)$ dimensional state vectors $\bar{u}_0(d(u)), \ldots, \bar{u}_{d(u,T(u))}(d(u))$ are strongly dependent mod p^s for all $s \geqslant T(u)$. By Lemma 2(b), this yields that $\bar{u}_0(d(u)), \ldots, \bar{u}_{d(u,T(u))}(d(u))$ are dependent over $\mathbb{Z}$. However, by Lemma 8, $\bar{u}_0(d(u)), \ldots, \bar{u}_{d(u)-1}(d(u))$ are independent, thus $d(u) \leqslant d(u, T(u))$. □

Lemma 10. *Let u be a l.r.s. and let $t \in \mathbb{N}$. Then there exist linear recurring sequences $u^{(1)}$ and $u^{(2)}$ such that $u = u^{(1)} + p^t u^{(2)}$, $T(u^{(1)}) \leqslant t$, $d(u^{(1)}) = d(u, t)$ and $d(u^{(2)}) \leqslant 2d(u)$.*

Proof. Let $u_n^{(1)} = u_n$ for $n = 0, \ldots, d(u,t) - 1$ and suppose that $u_n^{(1)}$ satisfies the recurrence relation

$$\bar{u}_n^{(1)}(d(u,t)) = M(u,t)^n \bar{u}_0^{(1)}(d(u,t)).$$

Since $u_n \equiv u_n^{(1)} \bmod p^t$, $v_p(u_n - u_n^{(1)}) \geqslant t$, and one can define $u_n^{(2)} = (u_n - u_n^{(1)})/p^t$. For these sequences $u = u^{(1)} + p^t u^{(2)}$ obviously holds. It is also clear that $T(u^{(1)}) \leqslant t$, and by Lemma 9, $d(u^{(1)}) = d(u^{(1)}, t) = d(u,t)$. By Lemma 6, $u^{(2)}$ is a l.r.s. with $d(u^{(2)}) \leqslant d(u^{(1)}) + d(u) \leqslant 2d(u)$. □

As we defined in Section 1, let $a_{s,0}, \ldots, a_{s,d(u,s)-1}$ be the defining coefficients corresponding to the minimal recurrence relation of $u \bmod p^s$. With this definition we have the following lemma:

Lemma 11. *Let u be a l.r.s. and suppose that $d(u,s) = d(u,s+k)$ for some $k \geqslant 0$. Then the minimal period length* $\bmod p^{k+1}$ *of the sequence defined by $a_{s+k,0}, \ldots, a_{s+k,d(u,s)-1}$ with initial values $b_0, \ldots, b_{d(u,s)-1}$ divides $\mu(u,s+k)$ for any $b_0, \ldots, b_{d(u,s)-1} \in \mathbb{Z}$.*

Proof. We will use the following notations: $\bar{u}_n = \bar{u}_n(d(u,s))$, $\mu = \mu(u,s+k)$ and $M = M(u,s+k)$.

By Lemma 7(a) and Remark 2, the $d(u,s)$ dimensional state vectors $\bar{u}_0, \ldots, \bar{u}_{d(u,s)-1}$ form a semi-basis $\bmod p^s$ and $\bmod p^{s+k}$. By Lemma 5, for every $\bar{b} \in \mathbb{Z}^{d(u,s)}$ there exist $\lambda_0, \ldots, \lambda_{d(u,s)-1} \in \mathbb{Z}$ such that

$$p^{s-1}\bar{b} \equiv \lambda_0 \bar{u}_0 + \cdots + \lambda_{d(u,s)-1}\bar{u}_{d(u,s)-1} \bmod p^{s+k}. \tag{6}$$

By the definition of μ, we have

$$\bar{u}_{n+\mu} \equiv \bar{u}_n \bmod p^{s+k},$$

i.e.

$$M^\mu \bar{u}_n \equiv \bar{u}_n \bmod p^{s+k}.$$

Substituting this into (6), we get

$$p^{s-1}\bar{b} \equiv p^{s-1} M^\mu \bar{b} \bmod p^{s+k},$$

whence

$$\bar{b} \equiv M^\mu \bar{b} \bmod p^{k+1}.$$

But this means that μ is a period length of the sequence defined by the coefficients $a_{s+k,0}, \ldots, a_{s+k,d(u,s)-1}$ with initial values $b_0, \ldots, b_{d(u,s)-1}$, and thus the minimal period length divides μ. □

Remark 4. Ward in Theorem 10.2 of [24] gave very similar result to our previous lemma.

Lemma 12. *Let u be a l.r.s., $s \geqslant T(u)$ and $l \in \mathbb{N}$. Then*

$$u_{n+l\mu(u,s)} - u_n \equiv l(u_{n+\mu(u,s)} - u_n) \bmod p^{s+1}.$$

Proof. Let $\bar{u}_n = \bar{u}_n(d(u))$, $\bar{y}_n = \bar{y}_n(d(u))$, $M = M(u)$, $\mu = \mu(u,s)$ and E the $d(u)$ dimensional unit matrix. Then

$$\begin{aligned}\bar{u}_{n+l\mu} - \bar{u}_n &\equiv (M^{l\mu} - E)\bar{u}_n \\ &\equiv \left(\sum_{i=0}^{l-1} M^{i\mu}\right)(M^{\mu} - E)\bar{u}_n \\ &\equiv \left(\sum_{i=0}^{l-1} M^{i\mu}\right)p^s \bar{y}_n \bmod p^{s+1} \qquad (7)\end{aligned}$$

with $y_n = (u_{n+\mu} - u_n)/p^s$ (the y_n are integers, since $u_n \equiv u_{n+\mu} \bmod p^s$). Thus we have $\bar{y}_n = M^{\mu}\bar{y}_0$ and by Lemma 9, $d(u,s) = d(u) = d(u,s+1)$. Hence by Lemma 11, $\mu(y,1)|\mu$, whence $M^{i\mu}\bar{y}_n \equiv \bar{y}_n \bmod p$. Substituting the last congruence into (7), we obtain the result. □

Lemma 13. *If $s \geqslant T(u)$, then either $\mu(u,s+1) = \mu(u,s)$ or $\mu(u,s+1) = p\mu(u,s)$.*

Proof. Define the sequence $y^{(l)}$ by $p^s y_n^{(l)} = u_{n+l\mu(u,s)} - u_n$, and put $\bar{y}_n^{(l)} = \bar{y}_n^{(l)}(d(u))$.

Suppose that $\mu(u,s+1) > \mu(u,s)$. This yields $\bar{y}_n^{(1)} \not\equiv 0 \bmod p$. By Lemma 12, $\bar{y}_n^{(l)} \equiv l\bar{y}_n^{(1)} \bmod p$, thus $\bar{y}_n^{(l)} \equiv 0 \bmod p$ if and only if $p|l$. From this, we get that the smallest positive value for l such that $u_{n+l\mu(u,s)} \equiv u_n \bmod p^{s+1}$ is $l = p$. □

Remark 5. Ward [22] in Theorem 7.1. claimed that for a third order l.r.s. the statement of Lemma 13 remains true even if we omit the condition $s \geqslant T(u)$. However, this is false, as shown e.g. by the sequence $u_n \bmod 5^s$, where u_n is defined by the recurrence relation $u_{n+3} = u_{n+2} + u_{n+1} + u_n$, with initial values $u_0 = 0$, $u_1 = 0$ and $u_2 = 5$. With this u we have $\mu(u,1) = 1$ and $\mu(u,2) = 31$.

Let us mention, that Theorem 11.1 of [24], which is a generalization of Theorem 7.1 in [22] is correct.

Lemma 14. *Let u be a l.r.s. and $s \geqslant 0$. Then $\mu(u,s) < p^{d(u)+s-1}$.*

Proof. Let v be the sequence satisfying the same recurrence relation as u with initial values $v_0 = 0, \ldots, v_{d(u)-2} = 0$, $v_{d(u)-1} = 1$. Then $\bar{v}_0(d(u)), \ldots, \bar{v}_{d(u)-1}(d(u))$ are linearly independent mod p, whence by Lemma 7(b), $d(u) \leqslant d(u,1)$. Thus $T(v) = 1$ and

by Lemma 13, we have $\mu(v,s)|\mu(v,1)p^{s-1}$. Since $\bar{u}_0(d(u))$ is a linear combination of the vectors $\bar{v}_0(d(u)),\ldots,\bar{v}_{d(u)-1}(d(u))$ (with integer coefficients), thus $\mu(u,s)|\mu(v,s)$. We know that $\mu(v,1)<p^{d(u)}$ whence $\mu(u,s)\leqslant\mu(v,s)\leqslant\mu(v,1)p^{s-1}<p^{d(u)}p^{s-1}$. □

Now we can prove a generalization of Lemma 12.

Lemma 15. *Let u and v be two linear recurring sequences, and $k\geqslant 0$. Suppose that there exists $T_0>T(u)$ such that $v_p(\mu(v,1+k+i))<v_p(\mu(u,T_0+i))$ for all $i\geqslant 0$. Set $\Lambda'=\mu(v,T(v))/\gcd(\mu(u,T_0),\mu(v,T(v))$ and $\Lambda=\Lambda'/p^{v_p(\Lambda')}$.*

Let $t\geqslant T_0$ and $s\geqslant T_0+k$ such that $\mu(u,s+1)=p\mu(u,s)$. Then for any $n,m,l,q\geqslant 0$

$$\begin{aligned}&(u+p^tv)_{n+m\mu(u,s)+ql\Lambda\mu(u,s+1)}-(u+p^tv)_{n+m\mu(u,s)}\\&\quad\equiv pl\Lambda(u_{n+q\mu(u,s)}-u_n)\bmod p^{s+k+1}\end{aligned}\tag{8}$$

holds.

Proof. The case $l=0$ is trivial.

Suppose that $l>0$. Let $M=M(u)*M(v)\in\mathbb{Z}^{d\times d}$, where $*$ denotes the operation defined after Remark 3 and d is the dimension of M. Further let E be the d dimensional unit matrix and write $\bar{u}_n=\bar{u}_n(d)$, $\bar{v}_n=\bar{v}_n(d)$, $\bar{y}_n=\bar{y}_n(d)$, $\mu_1=\mu(u,s)$ and $\mu_2=\mu(u,s+1)$. By similar arguments as in the proof of Lemma 12,

$$\begin{aligned}&(\bar{u}+p^t\bar{v})_{n+m\mu_1+lq\Lambda\mu_2}-(\bar{u}+p^t\bar{v})_{n+m\mu_1}\\&\quad\equiv M^{m\mu_1}(M^{lq\Lambda\mu_2}-E)(\bar{u}+p^t\bar{v})_n\\&\quad\equiv M^{m\mu_1}(M^{lq\Lambda p\mu_1}-E)\bar{u}_n+p^tM^{m\mu_1}(M^{lq\Lambda\mu_2}-E)\bar{v}_n\\&\quad\equiv M^{m\mu_1}\left(\sum_{i=0}^{l\Lambda p-1}M^{iq\mu_1}\right)(M^{q\mu_1}-E)\bar{u}_n+M^{m\mu_1}p^t(M^{lq\Lambda\mu_2}-E)\bar{v}_n\\&\quad\equiv\left(\sum_{i=0}^{l\Lambda p-1}M^{iq\mu_1}\right)M^{m\mu_1}p^s\bar{y}_n+M^{m\mu_1}p^t(M^{lq\Lambda\mu_2}-E)\bar{v}_n\bmod p^{s+k+1},\end{aligned}\tag{9}$$

with $y_n=(u_{n+q\mu_1}-u_n)/p^s$. (By definition of μ_1, y_n are integers.)

By Lemma 11,

$$M^{\mu_1}\bar{y}_n\equiv\bar{y}_n\bmod p^{k+1},\tag{10}$$

whence

$$\left(\sum_{i=0}^{pl\Lambda-1}M^{iq\mu_1}\right)\bar{y}_n\equiv pl\Lambda\bar{y}_n\bmod p^{k+1}.\tag{11}$$

Now we show that $M^{m\mu_1}p^t(M^{lq\Lambda\mu_2}-E)\bar{v}_n$ vanishes in congruence (9). We examine the following three cases:

(i) If $t > s+k$ then $p^t\bar{v}_n \equiv 0 \bmod p^{s+k+1}$.

(ii) If $s<t\leqslant s+k$, then

$$\mu(v, s+k+1-t)|\mu(v,k+1)|\Lambda\mu(u,T_0)|\Lambda\mu(u,s).$$

Hence $(M^{lq\Lambda\mu_2}-E)\bar{v}_n \equiv 0 \bmod p^{s+k+1-t}$.

(iii) Finally, if $t\leqslant s$, then by Lemma 13

$$\mu(v, s+k+1-t)|\Lambda\mu(u,T_0+s-t)|\Lambda\mu(u,s).$$

This proves that $M^{m\mu_1}p^t(M^{lq\Lambda\mu_2}-E)\bar{v}_n \equiv 0 \bmod p^{s+k+1}$. Applying the last assertion together with (11) and (10) to (9), we obtain the lemma. □

Corollary 2. *With the assumptions of Lemma* 15, *we have*

$$\begin{aligned}&(u+p^tv)_{n+lq\Lambda\mu(u,s+1)} - (u+p^tv)_n\\ &\quad\equiv l((u+p^tv)_{n+q\Lambda\mu(u,s+1)} - (u+p^tv)_n)\\ &\quad\equiv l\Lambda(u_{n+q\mu(u,s+1)} - u_n) \bmod p^{s+k+1}.\end{aligned}$$

Proof. By Lemma 15

$$\begin{aligned}&(u+p^tv)_{n+m\mu(u,s)+ql\Lambda\mu(u,s+1)} - (u+p^tv)_{n+m\mu(u,s)}\\ &\quad\equiv l(p\Lambda(u_{n+q\mu(u,s)} - u_n))\\ &\quad\equiv l((u+p^tv)_{n+q\Lambda\mu(u,s+1)} - (u+p^tv)_n) \bmod p^{s+k+1}.\end{aligned}$$

Set $v'=0$. Then

$$\begin{aligned}&(u+p^tv)_{n+m\mu(u,s)+ql\Lambda\mu(u,s+1)} - (u+p^tv)_{n+m\mu(u,s)}\\ &\quad\equiv l\Lambda(p(u_{n+q\mu(u,s)} - u_n))\\ &\quad\equiv l\Lambda((u+p^tv')_{n+q\mu(u,s+1)} - (u+p^tv')_n)\\ &\quad\equiv l\Lambda(u_{n+q\mu(u,s+1)} - u_n) \bmod p^{s+k+1}.\end{aligned}$$ □

Corollary 3. *Let u be a l.r.s. and* $s > T(u)$. *If* $\mu(u,s+1) = p\mu(u,s)$ *then* $\mu(u,s+2) = p\mu(u,s+1)$.

Proof. Let $\bar{u}_n = \bar{u}_n(d(u))$. Setting $k = 1$, $v_n = 0$, $m = 0$, $q = 1$ and $l = 1$ in Lemma 15 we obtain that

$$\bar{u}_{n+\mu(u,s+1)} - \bar{u}_n \equiv p(\bar{u}_{n+\mu(u,s)} - \bar{u}_n) \bmod p^{s+2}.$$

Since $\mu_{s+1} > \mu_s$, we have

$$\bar{u}_{n+\mu(u,s)} - \bar{u}_n \not\equiv 0 \bmod p^{s+1},$$

and thus

$$\bar{u}_{n+\mu(u,s+1)} - \bar{u}_n \not\equiv 0 \bmod p^{s+2}.$$

Hence by Lemma 13 we get $\mu_{s+2} = p\mu_{s+1}$. □

Remark 6. Ward in Theorem 11.1 of [24] proved a similar result to our Lemma 13 and Corollary 3.

Corollary 4. *Let u and v be linear recurring sequences over $\mathbb{Z}$ such that u is non-periodic, and let $k \in \mathbb{Z}$. Then there exists $T_0 \in \mathbb{Z}$ such that $v_p(\mu(v, 1+k+i)) < v_p(\mu(u, T_0+i))$ for all $i \geqslant 0$.*

Proof. For satisfying $v_p(\mu(v, 1+k+i)) < v_p(\mu(u, T_0+i))$ for all $i \geqslant 0$, it is enough to choose T_0 such that $\mu(u, T_0+1) = p\mu(u, T_0)$, $v_p(\mu(v, 1+k+i)) < v_p(\mu(u, T_0+i))$ for $0 \leqslant i \leqslant T(v)$. For $i > T(v)$ the property follows from Lemma 13 and Corollary 3. □

Remark 7. (a) By Lemma 14, $v_p(\mu(v, 1+k+i)) \leqslant d(v)+k+i-1$, and if we suppose that u is u.d. mod p^{T_0+i} then $T_0 + i \leqslant v_p(\mu(u, T_0+i))$. If $T_0 \geqslant d(v)+k$, then $v_p(\mu(v, 1+k+i)) \leqslant d(v)+1+k+i-2 < T_0+i \leqslant v_p(\mu(u, T_0+i))$.

(b) Further, again by Lemma 14, $v_p(\mu(u, T(u))) \leqslant d(u)+T(u)-2$. Thus $T_0 \leqslant v_p(\mu(u, T_0))$ provided that u is u.d. mod p^{T_0}. If $T_0 \geqslant d(u)+T(u)-1$ then $v_p(\mu(u, T(u))) \leqslant d(u)+T(u)-2 < T_0 \leqslant v_p(\mu(u, T_0))$. This yields that there exists an $i \in \mathbb{N}$ with $T(u) \leqslant i < T_0$ such that $v_p(\mu(u,i)) < v_p(\mu(u, i+1))$, whence by Lemma 13, $v_p(\mu(u,i)) + 1 \leqslant v_p(\mu(u, i+1))$. Using Corollary 3 we obtain by induction that $v_p(\mu(u, T_0)) + j \leqslant v_p(\mu(u, T_0+j))$ for all $j \geqslant 0$.

(c) Let $T' = \max\{d(v)+k, d(u)+T(u)-1\}$. If u is u.d. mod $p^{T'+1}$, then one can choose $T_0 = T'$ in Lemma 15.

Remark 8. Using the notations of Lemma 15, we find that $\mu(u + p^t v, s+1)$ divides $p\Lambda\mu(u,s)$, which comes from Corollary 3 and congruence (8) mod p^{s+1}.

Lemma 16. *Let u be a l.r.s., $s > T(u)+d(u)$, $l \geqslant 0$ such that $p \nmid l$ and suppose that $\mu(u,s) = p\mu(u, s-1)$. If $u_n \equiv u_{n+l\mu(u,s)} \bmod p^{s+d(u)}$ for some $0 \leqslant n$, then u cannot be u.d. mod $p^{s+d(u)}$.*

Proof. Setting $v_n = 0$, $T_0 = T(u)$ and $k = d(u)$, by Corollary 2

$$u_{n+l\mu(u,s)} - u_n \equiv l(u_{n+\mu(u,s)} - u_n) \bmod p^{s+d(u)}.$$

As $p \nmid l$, there exists l^{-1} such that $ll^{-1} \equiv 1 \bmod p^{s+d(u)}$. This yields

$$u_{n+m\mu(u,s)} - u_n \equiv ml^{-1}(u_{n+l\mu(u,s)} - u_n) \equiv 0 \bmod p^{s+d(u)},$$

for every $m \geqslant 0$. By Corollary 3 we know that $\mu(u, s + d(u)) = p^{d(u)}\mu(u, s)$. This means that $u_n, \ldots, u_{n+\mu(u,s+d(u))-1}$ contains at least $p^{d(u)}$ elements in the same residue class $\bmod p^{s+d(u)}$ as u_n.

Suppose that the sequence is uniformly distributed $\bmod p^{s+d(u)}$. Then among $u_n, \ldots, u_{n+\mu(u,s+d(u))-1}$, every residue class $\bmod p^{s+d(u)}$ appears with the same frequency. The number of different residue classes $\bmod p^{s+d(u)}$ is $p^{s+d(u)}$, thus $\mu(u, s + d(u)) \geqslant p^{s+d(u)}p^{d(u)} = p^{s+2d(u)}$. On the other hand, by Lemma 14, $\mu(u, s + d(u)) < p^{s+2d(u)-1}$, which is contradiction. □

Lemma 17. *Let u and v be two linear recurring sequences, T_0, t and Λ as in Lemma* 15 *and $s \geqslant T_0 + 2d(u)$. If u and $u + p^t v$ are u.d. $\bmod p^s$, then $u + p^t v$ is u.d. $\bmod p^{s+1}$.*

Proof. We will construct a partition $\mathfrak{H}$ of the set $\{0, \ldots, \Lambda\mu(u, s + 1) - 1\}$ such that if $A \in \mathfrak{H}$, then $u_n \equiv u_m \bmod p^s$ for all $n, m \in A$, and if $a \equiv b \bmod p^s$ then

$$\#\{n \in A | (u + p^t v)_n \equiv a \bmod p^{s+1}\} = \#\{n \in A | (u + p^t v)_n \equiv b \bmod p^{s+1}\}.$$

If one can find such a partition, then u and $u + p^t v$ are also uniformly distributed $\bmod p^{s+1}$.

Construct first the following class of sets:

$$A_{n,l} = \{i \mid i \equiv n \bmod \Lambda\mu(u, s - l) \text{ and } 0 \leqslant i < \Lambda\mu(u, s + 1)\},$$

where $0 \leqslant l < d(u)$ and $0 \leqslant n < \Lambda\mu(u, s - l)$.

Since $\mu(u, s + 1) = p^{l+1}\mu(u, s - l)$ by Remark 7(b), thus $\#A_{n,l} = p^{l+1}$ and $A_{n,l} = A_{m,r}$ if and only if $n = m$ and $l = r$.

Let

$$\mathfrak{H} = \{A_{n,l} \mid \forall i, j \in A_{n,l}\ u_i \equiv u_j \bmod p^s \text{ and}$$

$$\exists i, j \in A_{n,l} \text{ such that } u_i \not\equiv u_j \bmod p^{s+1}\}.$$

The proof works in two steps. In step (a) we will prove that $\mathfrak{H}$ is a partition of $\{0, \ldots, \Lambda\mu(u, s + 1) - 1\}$ and in step (b) we will prove that if $A_{n,l} \in \mathfrak{H}$ and

$a \equiv b \bmod p^s$, then

$$\#\{m \in A_{n,l} | (u + p^t v)_m \equiv a \bmod p^{s+1}\}$$
$$= \#\{m \in A_{n,l} | (u + p^t v)_m \equiv b \bmod p^{s+1}\}.$$

(a) We claim $\mathfrak{H}$ is a partition of $\{0, \ldots, \Lambda\mu(u, s+1) - 1\}$. For this we will prove the following:

(i) If $A_{n,l} \neq A_{m,r}$ and $A_{n,l} \cap A_{m,r} \neq \emptyset$, then $l < r$ and $A_{n,l} \subseteq A_{m,r}$ or $r < l$ and $A_{m,r} \subseteq A_{n,l}$.

Assume first that $l = r$. Then $A_{n,l} \cap A_{m,r} \neq \emptyset$ means that there exists an integer i such that $i \equiv n \bmod \Lambda\mu(u, s-l)$ and $i \equiv m \bmod \Lambda\mu(u, s-l)$, and consequently $m \equiv n \bmod \Lambda\mu(u, s-l)$. But $0 \leqslant n,\ m < \Lambda\mu(u, s-l)$, whence $n = m$ and $A_{n,l} = A_{m,r}$.

If $l \neq r$ then we may assume without loss of generality that $l < r$. In this case $A_{n,l} \cap A_{m,r} \neq \emptyset$ means that there exists an integer i such that $i \equiv n \bmod \Lambda\mu(u, s-l)$ and $i \equiv m \bmod \Lambda\mu(u, s-r)$ and since $\mu(u, s-r) | \mu(u, s-l)$, thus $m \equiv n \bmod \Lambda\mu(u, s-r)$. Let $j \in A_{n,l}$. Then $j \equiv n \bmod \Lambda\mu(u, s-l)$ and consequently $j \equiv n \equiv m \bmod \Lambda\mu(u, s-r)$, thus $A_{n,l} \subseteq A_{m,r}$.

(ii) If $A_{m,r} \in \mathfrak{H}$ then no proper subsets of $A_{m,r}$ are elements of $\mathfrak{H}$.

Suppose that $A_{m,r} \in \mathfrak{H}$ and $A_{n,l} \subsetneq A_{m,r}$. By (i), $l < r$. Let m' be such that $m' \equiv n \bmod \Lambda\mu(u, s-r+1)$ and $0 \leqslant m' < \Lambda\mu(u, s-r+1)$.

We will show that $A_{n,l} \subseteq A_{m',r-1} \subsetneq A_{m,r}$. By the definition of m' and $A_{m',r-1}$ we know that $n \in A_{m',r-1}$ which means that $A_{m',r-1} \cap A_{n,l} \neq \emptyset$, and by (i), $A_{n,l} \subseteq A_{m',r-1}$. This yields that $A_{m',r-1} \cap A_{m,r} \neq \emptyset$ and again by (i), $A_{m',r-1} \subseteq A_{m,r}$. Since $\#A_{m',r-1} \neq \#A_{m,r}$, thus $A_{m',r-1} \subsetneq A_{m,r}$.

We claim that if $i \in A_{n,l}$, then $u_i \equiv u_{m'} \bmod p^{s+1}$.

Let $i \in A_{n,l}$. Since $A_{n,l} \subseteq A_{m',r-1}$, thus $i \in A_{m',r-1}$ and there exists an integer a such that $i = m' + a\Lambda\mu(u, s-r+1)$. If we set $v_n = 0$, $k = d(u)$, $l = a$ and $q = \Lambda$, by Lemma 15 we obtain

$$u_i - u_{m'} \equiv pa(u_{m'+\Lambda\mu(u,s-r)} - u_{m'}) \bmod p^{s-r+d(u)+1},$$

whence

$$u_i - u_{m'} \equiv pa(u_{m'+\Lambda\mu(u,s-r)} - u_{m'}) \bmod p^{s+1}.$$

Since $A_{m',r-1} \subseteq A_{m,r}$ and $0 \leqslant m' + \Lambda\mu(u, s-r) \leqslant i < \Lambda\mu(u, s+1)$, thus $m', m' + \Lambda\mu(u, s-r) \in A_{m,r}$. But $A_{m,r} \in \mathfrak{H}$, whence $u_{m'} \equiv u_{m'+\Lambda\mu(u,s-r)} \bmod p^s$. This yields $p(u_{m'+\Lambda\mu(u,s-r)} - u_{m'}) \equiv 0 \bmod p^{s+1}$, i.e. $u_i \equiv u_{m'} \bmod p^{s+1}$. Hence, $u_i \equiv u_{m'} \equiv u_j \bmod p^{s+1}$ for every $i, j \in A_{n,l}$, thus $A_{n,l} \notin \mathfrak{H}$.

(iii) Finally, we prove that

$$\bigcup_{A \in \mathfrak{H}} A = \{0, \ldots, \Lambda\mu(u, s+1) - 1\}.$$

During step (iii) we will use the notation $d = d(u)$ and $\mu(i) = \mu(u, s-d+1+i)$.

We will create a sequence of partitions $\mathfrak{H}_0, \mathfrak{H}_1, \ldots$ such that

$$\bigcup_{A\in\mathfrak{H}_i} A = \{0, \ldots, \Lambda\mu(u, s+1) - 1\},$$

$\mathfrak{H}_{i+1}$ is a refinement of $\mathfrak{H}_i$ and $\mathfrak{H} = \mathfrak{H}_{d-1}$. (Actually we will not need that every $\mathfrak{H}_i$ is a partition of $\{0, \ldots, \Lambda\mu(u, s+1) - 1\}$, but obviously they are.)

Let $\mathfrak{H}_0 = \{A_{n,d-1} \mid 0 \leqslant n < \Lambda\mu(0)\}$. Assuming we already defined $\mathfrak{H}_i$, we define $\mathfrak{H}_{i+1}$ by the following:

Let

$$\mathfrak{H}_i' = \{A \mid A\in\mathfrak{H}_i \text{ and } \exists j_1, j_2 \in A\colon u_{j_1} \not\equiv u_{j_2} \bmod p^s\}$$

and let

$$\mathfrak{H}_{i+1} = (\mathfrak{H}_i \backslash \mathfrak{H}_i') \cup \bigcup_{A_{n,r}\in\mathfrak{H}_i'} \{A_{n+a\Lambda\mu(u,s-r),r-1} \mid 0 \leqslant a < p\}.$$

Simple observation shows that the elements of $\mathfrak{H}_i'$ have the form $A_{n,d-1-i}$.

First we prove that

$$\bigcup_{A\in\mathfrak{H}_i} A = \{0, \ldots, \Lambda\mu(u, s+1) - 1\}$$

for all $i \geqslant 0$.

Obviously if $i = 0$, the property holds.

Suppose that

$$\bigcup_{A\in\mathfrak{H}_i} A = \{0, \ldots, \Lambda\mu(u, s+1) - 1\}.$$

Since $s - d + 1 + i \geqslant T_0 + d \geqslant T(u) + d$ for every $0 \leqslant i \leqslant d-1$, by similar considerations as in Remark 7(b), we have

$$\mu(i+1) = p\mu(i), \tag{12}$$

whence

$$\bigcup_{a=0}^{p-1} A_{n+a\Lambda\mu(i),d-2-i} = A_{n,d-1-i}.$$

(All the sets $A_{n+a\Lambda\mu(i),d-2-i}$ are different, all of them is a subset of $A_{n,d-1-i}$ and comparing the cardinalities we get the equality.) Hence

$$\bigcup_{A\in\mathfrak{H}_{i+1}} A = \{0, \ldots, \Lambda\mu(u, s+1) - 1\}.$$

Now we prove that if $i \geqslant 0$ and $A \in \mathfrak{H}_i$, then there exist $j_1, j_2 \in A$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^{s+1}$.

First let $i = 0$. Since u is u.d. $\bmod p^s$ and (12) holds, by Lemma 16

$$u_n \not\equiv u_{n+\Lambda\mu(0)} \bmod p^{(s-d+1)+d}$$

for every $0 \leqslant n < \Lambda\mu(0)$. This means that for every $A_{n,d-1} \in \mathfrak{H}_0$ there exist $j_1, j_2 \in A_{n,d-1}$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^{s+1}$ (e.g. $j_1 = n$ and $j_2 = n + \Lambda\mu(0)$).

Suppose now that $\mathfrak{H}_i$ has the required property. If $A \in \mathfrak{H}_i \cap \mathfrak{H}_{i+1}$, then obviously there exist $j_1, j_2 \in A$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^{s+1}$.

Therefore assume that $A \in \mathfrak{H}_{i+1} \setminus \mathfrak{H}_i$. This yields that $A = A_{n,d-2-i}$ for some $0 \leqslant n < \Lambda\mu(i+1)$. Let m be such that $n \equiv m \bmod \Lambda\mu(i)$ and $0 \leqslant m < \Lambda\mu(i)$. For this m we have $A_{m,d-1-i} \in \mathfrak{H}_i \setminus \mathfrak{H}_{i+1}$.

By the definition of $\mathfrak{H}_{i+1}$ there exist $j_1, j_2 \in A_{m,d-1-i}$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^s$.

Fix $j_1, j_2 \in A_{m,d-1-i}$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^s$, a_1, a_2 such that $j_1 = m + a_1\Lambda\mu(i)$ and $j_2 = m + a_2\Lambda\mu(i)$, and set $v = 0$ and $k = d$. Then by Corollary 2

$$\begin{aligned} u_{j_1} - u_{j_2} &= (u_{j_1} - u_m) - (u_{j_2} - u_m) \\ &\equiv a_1(u_{m+\Lambda\mu(i)} - u_m) - a_2(u_{m+\Lambda\mu(i)} - u_m) \\ &= (a_1 - a_2)(u_{m+\Lambda\mu(i)} - u_m) \bmod p^{(s-d+i)+d+1}, \end{aligned}$$

whence

$$u_{m+\Lambda\mu(i)} \not\equiv u_m \bmod p^s \tag{13}$$

follows.

Setting $v = 0$, $k = d$ and $l = 1$ in Lemma 15, congruence (8) will have the form

$$u_{n+m\mu(u,s)+q\mu(u,s+1)} - u_{n+m\mu(u,s)} \equiv p(u_{n+q\mu(u,s)} - u_n) \bmod p^{s+k+1}.$$

We remark, that the symbol Λ used in Lemma 15 will have the value 1, while the symbol T_0 can be chosen to be equal to $T(u) + 1$. Here the condition for s is

$$s \geqslant T_0 + k = T(u) + 1 + d.$$

We can use the above form of (8) here, substituting the present value of Λ into the original symbol q, the present value of m into the original symbol n and the present value of $s - d + 1 + i$ into the original s.

We should remark, that

$$s - d + 1 + i \geqslant T(u) + 2d - d + 1 + i \geqslant T(u) + d + 1,$$

and the present value of n is a substitution of the original $n + m\mu(u, s)$.

Thus

$$u_{n+\Lambda\mu(i+1)} - u_n \equiv p(u_{m+\Lambda\mu(i)} - u_m) \bmod p^{(s-d+1+i)+d+1},$$

and by (13) we obtain

$$u_{n+\Lambda\mu(i+1)} \not\equiv u_n \bmod p^{s+1},$$

whence there exist $j_1, j_2 \in A_{n,d-2-i}$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^{s+1}$ (e.g. $j_1 = n$ and $j_2 = n + \Lambda\mu(i+1)$).

Finally, we have to prove only that $\mathfrak{H}_{d-1} = \mathfrak{H}$.

Let $i = d-1$. Then for every $A \in \mathfrak{H}_{d-1}$ there exist $j_1, j_2 \in A$ such that $u_{j_1} \not\equiv u_{j_2} \bmod p^{s+1}$. Further, by the definition of $\mu(u,s)$, we know that $u_{n+\mu(u,s)} - u_n \equiv 0 \bmod p^s$, i.e. $u_{j_1} \equiv u_{j_2} \bmod p^s$ for all $j_1, j_2 \in A_{n,0}$. If $A_{n,d-1-i} \in \mathfrak{H}_{d-1}$, where $0 \leqslant i < d-1$, then $A_{n,d-1-i} \in \mathfrak{H}_{d-2}$, too, and by the definition of $\mathfrak{H}_{d-1}$, we have $u_{j_1} \equiv u_{j_2} \bmod p^s$ for all $j_1, j_2 \in A_{n,d-1-i}$.

Hence $\mathfrak{H}_{d-1} = \mathfrak{H}$ and thus

$$\bigcup_{A \in \mathfrak{H}} A = \{0, \ldots, \Lambda\mu(u, s+1) - 1\}.$$

(b) Now we turn to the assertion, that if $A \in \mathfrak{H}$ and $a \equiv b \bmod p^s$, then

$$\#\{n \in A \mid (u + p^t v)_n \equiv a \bmod p^{s+1}\}$$

$$= \#\{n \in A \mid (u + p^t v)_n \equiv b \bmod p^{s+1}\}.$$

Let $A = A_{m,r}$, $n \in A_{m,r}$ and a be such that $n = m + a\Lambda\mu(u, s-r)$. Setting $k = d(u)$, by Corollary 2

$$(u + p^t v)_n - (u + p^t v)_m \equiv a(u_{m+\Lambda\mu(u,s-r)} - u_m) \bmod p^{(s-r-1)+d(u)+1}.$$

Since $A_{m,r} \in \mathfrak{H}$, thus $u_{m+\Lambda\mu(u,s-r)} - u_m \equiv 0 \bmod p^s$, but $u_{m+\Lambda\mu(u,s-r)} - u_m \not\equiv 0 \bmod p^{s+1}$.

Let $y_m = (u_{m+\Lambda\mu(u,s-r)} - u_m)/p^s$. Since $r < d(u)$, thus

$$(u + p^t v)_n - (u + p^t v)_m \equiv a\Lambda p^s y_m \bmod p^{s+1},$$

i.e.

$$(u + p^t v)_n \equiv a\Lambda p^s y_m + (u + p^t v)_m \bmod p^{s+1}.$$

Since $y_m \not\equiv 0 \bmod p$, thus $(u + p^t v)_{n_1} \equiv (u + p^t v)_{n_2} \bmod p^{s+1}$ if and only if the corresponding a_1, a_2 are such that $a_1 \equiv a_2 \bmod p$.

We know that $A_{m,r}$ has p^{r+1} elements, which yields that a takes values from $[0, p^{r+1} - 1]$. Since every residue class $\bmod p$ appears p^r times in $[0, p^{r+1} - 1]$, thus all the residue classes $\bmod p^{s+1}$ which appear in $\{(u + p^t v)_n \mid n \in A_{m,r}\}$ have p^r representatives, and thus the assertion is proved. □

Corollary 5. *Let u and v be two l.r.s., T_0 and Λ as in Lemma* 15, $s > T_0 + 2d(u)$ *and* $t \geqslant T(u) + 2d(u)$. *If* $u + p^t v$ *is u.d.* $\bmod p^s$, *then* $u + p^t v$ *is u.d.* $\bmod p^{s+1}$.

Proof. Let $v' = 0$. Then the corresponding T_0' can be chosen to be equal to $T(u) + 1$. We will use in the lemma the fact, that if a sequence is uniformly distributed modulo an integer, then it is uniformly distributed modulo every divisor of this integer.

If $s < t$, then $u + p^t v \equiv u \bmod p^{s+1}$. Since $T_0 > T(u)$ and $u + p^t v'$ are u.d. modulo p^s, thus by Lemma 17, $u + p^t v'$ is also u.d. modulo p^{s+1}. But

$$u + p^t v' \equiv u \equiv u + p^t v \bmod p^{s+1},$$

whence the statement of the corollary follows.

If $s \geqslant t$, then since $u + p^t v \equiv u \bmod p^t$, thus u is u.d. modulo p^t.

Since $t \geqslant T(u) + 2d(u)$, applying Lemma 17 and supposing that u and $u + p^t v'$ are u.d. modulo p^t, then $u + p^t v' = u$ is u.d. modulo p^{t+1}.

Hence by induction u is u.d. modulo p^s, whence again by Lemma 17, the statement follows. □

Lemma 18. *Let u be a l.r.s. with $d(u) \geqslant 2$. Then there exists an integer $t \geqslant 0$ and two linear recurring sequences $u^{(1)}$ and $u^{(2)}$ such that $u = u^{(1)} + p^t u^{(2)}$, $d(u^{(1)}) \leqslant d(u)$,*

$$T(u^{(1)}) \leqslant \frac{3d(u^{(1)})^2 + d(u^{(1)})}{2} + 2 + d(u)$$

and

$$\max\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\} < t.$$

Proof. Let $T_1, \ldots, T_m$ be such that $T_1 = 1$, $T_m = T(u)$ and $d(u, T_{i+1}) > d(u, T_{i+1} - 1) = d(u, T_i)$ for all $1 \leqslant i < m$. Let i be fixed. By Lemma 10 there exist $v^{(1,i)}$ and $v^{(2,i)}$ such that $u = v^{(1,i)} + p^{T_{i+1}-1} v^{(2,i)}$, $T(v^{(1,i)}) \leqslant T_{i+1} - 1$ and $d(v^{(1,i)}) = d(u, T_{i+1} - 1) = d(u, T_i)$.

Since $v_n^{(1,i)} \equiv u_n \bmod p^t$ for all $n \geqslant 0$ and $0 \leqslant t \leqslant T_{i+1} - 1$, it follows that $d(v^{(1,i)}, t) = d(u, t)$ for all $0 \leqslant t \leqslant T_{i+1} - 1$, whence $T(v^{(1,i)}) = T_i$.

Now suppose that there exists an $1 \leqslant i < m$ such that

$$\max\{T_i + 3d(v^{(1,i)}) - 1, 4d(v^{(1,i)}) + d(u)\} < T_{i+1}$$

and fix i to be the smallest positive integer with the previous property. Further suppose that there exists an $1 < l \leqslant i$ integer such that

$$T_{l-1} + 3d(v^{(1,l-1)}) - 1 < T_l \tag{14}$$

and fix l to be the maximal with this property.

Then

$$T_i \leqslant T_l + \sum_{j=l}^{i-1} (3d(v^{(1,j)}) - 1). \tag{15}$$

Since $d(v^{(1,j)}) \leqslant d(v^{(1,i-1)})$ for all $j<i$ and $d(v^{(1,l-1)}) < d(v^{(1,l)})$, it follows that

$$\begin{aligned}
&\sum_{j=l}^{i-1} (3d(v^{(1,j)}) - 1) \\
&\quad \leqslant \sum_{j=d(v^{(1,l)})}^{d(v^{(1,i-1)})} (3j-1) \\
&\quad = \frac{(3d(v^{(1,i-1)}) - 1 + 3d(v^{(1,l)}) - 1)(d(v^{(1,i-1)}) - d(v^{(1,l)}) + 1)}{2} \\
&\quad = \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 5d(v^{(1,l)}) - 2}{2}.
\end{aligned}$$

By the definition of i and l, it follows that $T_l \leqslant 4d(v^{(1,l-1)}) + d(u)$. Since $d(v^{(1,l-1)}) \leqslant d(v^{(1,l)}) - 1$, thus

$$\begin{aligned}
T_i &\leqslant d(u) + 4(d(v^{(1,l)}) - 1) \\
&\quad + \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 5d(v^{(1,l)}) - 2}{2} \\
&= d(u) + \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 13d(v^{(1,l)}) - 10}{2}.
\end{aligned}$$

This expression, as a quadratic expression of $d(v^{(1,l)})$, has an absolute maximum at $d(v^{(1,l)}) = 2$, whence $T_i \leqslant d(u) + (3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) + 4)/2$.

If $1<l\leqslant i$ does not exist with property (14), then set $l = 1$ in (15). Since $T_1 = 1$, the previous upper bound for T_i is still valid. For this i we can define $u^{(1)} = v^{(1,i)}$, $u^{(2)} = v^{(2,i)}$ and $t = T_{i+1} - 1$.

If there are no i satisfying

$$\max\{T_{i-1} + 3d(v^{(1,i-1)}) - 1, 4d(v^{(1,i-1)}) + d(u)\} < T_i,$$

then either $T(u) \leqslant 5d(u)$ or if $T_j > 4d(v^{(1,j)}) + d(u)$, then $T_j \leqslant T_{j-1} + 3d(v^{(1,j-1)}) - 1$ for all $1<j\leqslant m$. In both cases we may choose $u^{(1)} = u$, $u^{(2)} = 0$ and $t = T(u) + 5d(u)$. □

4. Proof of the theorem

Suppose first that u is not purely periodic mod p^s for some $s \geqslant 0$ and let $\mu_s > 0$ such that $u_{\mu_s+\mu(u,s)+n} \equiv u_{\mu_s+n} \bmod p^s$ for every $n \geqslant 0$. Further, let $v_n^{(s)} = u_{\mu_s+n}$. Clearly $v^{(s)}$ is purely periodic mod p^s and $v^{(s)}$ is u.d. mod p^s if and only if u is u.d. mod p^s. Thus, to prove that u is u.d. mod p^s, it is enough to show that $v^{(s)}$ is u.d. mod p^s.

Therefore, without loss of generality, we may suppose that for a fixed, but arbitrarily big $s' \geqslant 0$, the sequence u is purely periodic mod $p^{s'}$.

If $s \leqslant S$ then u is obviously u.d. mod p^s. Suppose that $s \geqslant S$ and u is u.d. mod p^s. By Lemma 18, u can be split such that $u = u^{(1)} + p^t u^{(2)}$, where

$$d(u^{(1)}) \leqslant d(u),$$

$$\begin{aligned} T(u^{(1)}) &\leqslant \frac{3d(u^{(1)})^2 + d(u^{(1)})}{2} + 2 + d(u) \\ &\leqslant 3\frac{d(u)^2 + d(u)}{2} + 2 \end{aligned}$$

and

$$t > \max\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\}.$$

Hence

$$\begin{aligned} s \geqslant S &= \frac{3d(u)^2 + 9d(u)}{2} + 1 \\ &\geqslant \max\left\{3\frac{d(u)^2 + d(u)}{2} + 2 + 3d(u) - 1, 5d(u)\right\} \\ &\geqslant \max\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\}. \end{aligned}$$

Let

$$T' = \max\{d(u^{(2)}) + d(u^{(1)}), d(u^{(1)}) + T(u^{(1)}) - 1\}.$$

Since $u^{(2)}$ is a linear combination of $u^{(1)}$ and u, thus by Lemma 6,

$$\begin{aligned} T' &= \max\{d(u^{(2)}) + d(u^{(1)}), d(u^{(1)}) + T(u^{(1)}) - 1\} \\ &\leqslant \max\{d(u) + 2d(u^{(1)}), d(u^{(1)}) + T(u^{(1)}) - 1\} < s, \end{aligned}$$

consequently u is u.d. modulo $p^{T'+1}$. Since $T' < t$, we have

$$u^{(1)} \equiv u \bmod p^{T'+1}$$

and thus $u^{(1)}$ is u.d. modulo $p^{T'+1}$.

Hence, setting $k = d(u^{(1)})$, by Remark 7, we can choose $T_0 = T'$. Thus

$$T_0 + 2d(u^{(1)}) \leqslant \max\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\} \leqslant s.$$

Similarly, $T_0 + 2d(u^{(1)}) \leqslant t$, whence by Corollary 5, $u = u^{(1)} + p^t u^{(2)}$ is u.d. modulo p^{s+1}.

Since s is arbitrary, we obtain the theorem by induction. □

Remark. By a detailed analysis of the results, in special cases one can obtain much better bounds than in the general case.

For instance, if $T(u) = 1$, which is rather often the case, it is enough if $s \geqslant 3d(u) + 1$.

Acknowledgments

I should thank the referee for his very careful reading and correcting the manuscript. I am also grateful for his valuable remarks, which helped me to refine the clarity and precision of the presentation.

References

[1] T.S. Blyth, Module Theory, Oxford University Press, Oxford, 1977.
[2] R.T. Bumby, A distribution property for linear recurrence of the second order, Proc. Amer. Math. Soc. 50 (1975) 101–106.
[3] P. Bundschuh, J. Shiue, Solution of a problem on the uniform distribution of integers, Atti Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Nat. 55 (1973) 172–177.
[4] P. Bundschuh, On the distribution of Fibonacci numbers, Tamkang J. Math. 5 (1974) 75–79.
[5] W. Carlip, E. Jacobson, A criterion for stability of two-term recurrence sequences modulo 2^k, Finite Fields Appl. 2 (1996) 369–406.
[6] M. Drmota, R.F. Tichy, Sequences, Discrepancies and Applications, Vol. 1651, Lecture Notes in Mathematics, Springer, New York, 1997.
[7] H.J.A. Duparc, Periodicity properties of recurring sequences. I, Nederl. Akad. Wet., Proc. Ser. A 57 (1954) 331–342.
[8] H.J.A. Duparc, Periodicity properties of recurring sequences. II, Nederl. Akad. Wet., Proc. Ser. A 57 (1954) 473–485.
[9] T. Herendi, Linear recurring sequences, Ph.D. Thesis, Debrecen, 2002.
[10] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, Cambridge, 1986.
[11] W. Narkiewicz, Uniform Distribution of Sequences of Integers in Residue Classes, Vol. 1087, Lecture Notes in Mathematics, Springer, New York, 1984.

[12] M.B. Nathanson, Linear recurrences and uniform distribution, Proc. Amer. Math. Soc. 48 (2) (1975) 289–291.
[13] H. Niederreiter, Distribution of Fibonacci numbers mod 5^k, Fibonacci Quart. 10 (4) (1972) 373–374.
[14] H. Niederreiter, J.S. Shiue, Equidistribution of linear recurring sequences in finite fields, Indag. Math. 39 (1977) 397–405.
[15] H. Niederreiter, J.S. Shiue, Equidistribution of linear recurring sequences in finite fields. II, Acta Arith. 38 (1981) 197–207.
[16] T.N. Shorey, R. Tijdeman, Exponential Diophantine Equations, in: Cambridge Tracts in Mathematics, Vol. 87, Cambridge University Press, Cambridge, 1986.
[17] L. Sommer, W. Carlip, Stability of second-oder recurrences modulo p^r, Internat. J. Math. Math. Sci. 23 (2000) 225–241.
[18] R.F. Tichy, G. Turnwald, Uniform distribution of recurrences in Dedekind domains, Acta Arith. 46 (1985) 81–89.
[19] R.F. Tichy, Contributions to general algebra 5, Proceedings of the Salzburg Conference, Mai 29- June 1, 1986, Verlag Hoelder-Pichler-Tempsky, Wien, Verlag B.G. Teubner, Stuttgart, 1987, pp. 401–406.
[20] G. Turnwald, Gleichverteilung von linearen rekursiven Folgen, Sitzungber., Abt. II, Oesterr. Akad. Wiss., Math.-Naturwiss. 193 (1985) 201–245.
[21] G. Turnwald, Uniform distribution of second-order linear recurring sequences, Proc. Amer. Math. Soc. 96 (2) (1986) 189–198.
[22] M. Ward, The characteristic number of a sequence of integers, satisfying a linear recursion relation, Trans. Amer. Math. Soc. 33 (1931) 153–165.
[23] M. Ward, The distribution of residues in sequences satisfying a linear recurrence relation, Trans. Amer. Math. Soc. 33 (1931) 166–190.
[24] M. Ward, The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. 35 (1933) 600–628.
[25] W.A. Webb, C.T. Long, Distribution modulo p^k of the general linear second order recurrence, Atti Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Nat. 58 (1975) 92–100.